St. Peter’s Church, Wellesbourne

Data Protection policy

Contents

Policy summary

St Peter's uses personal information to carry out its' many functions supporting the mission and ministry of the Church of England. St Peter's therefore collects a wide range of personal data required in order to carry out these functions including employees, those involved in pastoral care, baptism, weddings, funerals, gift aid and so on.

St Peter's will endeavour to ensure that it uses personal information in line with the expectations and interests of those with whom they come into contact including employees, office holders and others, for the benefit of the church and wider society and in compliance with data protection legislation.

This policy provides guidance of personal data (collection, use, storage, sharing and disposal) in accordance with the data protection legislation. It applies to data that relates to identifiable living individuals stored and used either electronically or on paper. Compliant processing will support effective business operations and minimise the risk of harm to individuals.

Adherence to this policy is mandatory for all at St Peter's including employees, contractors, volunteers and those who hold personal data.

Introduction

As from 25th May 2018, the General Data Protection Regulation (GDPR) became law and replaced the Data Protection Act 1998. However there are two additional requirements to the existing act:

- The emphasis on the rights on the individual to control what the organisation is doing in regard to personal data
- Emphasis on transparency and accountability

Policy statement

Personal data that St Peter's collects, uses, stores, transfers, shares and disposes of must be handled in line with the principles outlined below regarding data protection.

Responsibility

The PCC are responsible for:

- Approval and implementation of this policy
- Appointing a data protection lead
- Ensuring data controllers are signed up to this policy and aware that they protect the information they create
- All data controllers knowing what to do in case of a breach
- Appointing a data protection team to advise on best practice, provide guidance, provide training if required and support the data protection officer
- Completing the GDPR checklist (appendix 1)

Purpose

The purpose of this policy is to set out relevant legislation and to describe the steps that St Peter's will take to be compliant.

This requires checks to be made:

- To establish what personal data is being held, why and with whom it is being shared
- To establish where and how this personal data is being stored and who has access to it
- To establish if such storage can be justified, is fully processed with a consent and privacy notice and this is fully documented
- To review all retention periods and discern if these are justified.
- Ensure there is a robust system for deleting or destroying personal data
- Ensure a breach management procedure is in place.

Ensuring best practice

The GDPR makes clear that protection of data must be considered when deciding what personal data you need and how you're going to process it, collect it, store it, share it and dispose of it.

All those at St Peter's processing personal data on behalf of the organisation including employees, volunteers, suppliers, partners, contractors and agents are required to act in accordance with this policy. Failure to comply could result in disciplinary action for employees and those mentioned above.

Data controller

This is an organisation or individual who makes decisions about how personal data is being processed. In the case of St. Peter's Church, the Vicar is the data controller for pastoral care and the Chairman of the PCC for administration.

Accountability

Transparency, openness and accountability are key components of the GDPR and any organisation, if scrutinized, must be able to show they are compliant with the legislation; this includes St Peter's. Therefore due process must be followed about how a decision has been made to establish if, how and where, personal data can be kept.

Article 6 of the GDPR sets out various legal bases for the processing of personal data for legitimate business which include:

- Legal obligation eg processing gift aid, electoral roll information
- Legitimate interest eg administration of church groups – rotas
- Consent eg sending out invitations to specific events
- Contract eg hirer's agreement for church centre and church

There are also special categories of personal data under GDPR about religious beliefs. Refer to article 6 of the Church of England GDPR document.

St. Peter's must ensure that the most appropriate and most secure methods are available for both storage and disposal. St Peter's should ensure that:

- In so far as possible, all personal data in its' possession (either in the Parish Administrator's office or with data controllers) is kept secure from unauthorised access
- Physical files containing personal data are locked in a secure cabinet
- There is vigilance particularly when taking, eg. files, laptops off site, that they are not left in a position where they could be stolen or lost
- All devices used to handle personal data are password protected and the password is not shared with anyone unauthorised to use it
- No personal data is placed, eg Administrator's office, where it can be accessed.

The data protection lead (Vicar) can advise if you are unsure if you are compliant with the GDPR.

Privacy and Consent notices

Having first considered the need to retain personal data and the mechanisms for this, a privacy notice needs to be issued to the individual with a consent form (appendices 2 and 3). The individual needs to read the privacy notice, complete the consent form and return it to the Parish Office. This is then kept on file as a hard copy in a locked cabinet in the inner office of the Parish Administrator's office. An electronic copy as a working document of all who have given consent is stored on a password protected Dropbox file on the Parish Office computer. In the home situation the individual needs to check that any storage they need to keep for working purposes has been consented and that storage is password protected. The Parish Administrator needs to know who is storing personal data and on whom. Such individuals will be known as data controllers.

Personal data can only be used for the purposes for which consent has been given.

If you obtain personal data from other sources, then a privacy notice needs to be issued within a reasonable period of time and consent obtained.

Legitimate interest test

Legitimate interest is the reason for securing and using personal data without obtaining consent. You can rely on legitimate interest when:

- Processing is not required by law but is of benefit to you
- There is a limited privacy impact on the data subject
- The data subject would reasonably expect your processing to take place.

In order to use legitimate interest as a lawful basis for processing, it must meet the following criteria:

- Have a specific purpose with a defined benefit
- Be necessary
- Be balanced against and not override the interest, rights and freedoms of data subjects

If unsure, an assessment can be carried out. It is essential that this should be completed for all employees (appendix 5)

Criminal offence data

This is personal data relating to criminal convictions and offences. Further guidance can be found in The Church of England data protection policy

Individual rights

The GDPR includes the following rights for individuals:

- The right to be informed (usually through a privacy notice), but also if required, the organisation needs to be able to explain the lawful basis for the processing of the individual's data, data retention period, who it will be shared with and the right to complain.
- The right to access how personal data is being stored and used. Requests must be responded to within one month. It is possible to refuse to comply with the request especially if the individual is making repetitive, excessive or manifestly unfounded requests. If a request is refused, the Information Governance Officer needs to be informed at the Diocese.
- The right to rectification if information is inaccurate or incomplete. It is St. Peter's responsibility to inform and ask for correction where they have given data to a third party
- The right to erasure. The individual has the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. St Peter's does not have to agree to the request, for example regarding the retention of safeguarding records or financial information for gift aid
- The right to restrict processing ie to restrict how personal data is used particularly until a dispute can be settled
- The right to data portability. This is highly unlikely to affect St Peter's
- The right to object eg an individual might not agree on a legitimate interest reason for processing personal data
- The right not to be subject to automated decision-making including profiling. This protects the individual from the risk of a potentially damaging decision being made without human intervention.

Processing personal data about children

If St Peter's offers online services directly to children and relies on consent to collect their information, then parent/guardian consent is required to lawfully use this data. This applies to children 13 years and under. Any privacy notice or consent documents issued to children/young adults must be in a language that a child can understand. Such records must be retained in a secure filing cabinet. (Refer to the safeguarding policy.)

Data protection impact assessment

It is unlikely such an assessment will be required for St Peter's but if a large project was to be undertaken it may be good practice to do one. See Church of England resources for further information.

Disclosure

It is an offence for any person to knowingly or recklessly, without consent of St Peter's to:

- Obtain or disclose personal data or the information contained in personal data or
- Procure the disclosure to another person of the information contained in personal data or
- Retain personal data without the consent of the data controller who procured it.

UNLESS the disclosure was:

- Necessary for the purpose of preventing or detecting a crime
- Required by the order of a court or tribunal or authorised by law
- Justified as being in the public interest
- Based on the belief that you had a legal right to obtain, disclose or retain the data
- Based on the belief that the data controller would have consented if they had known

If you are asked to disclose personal data in an emergency and are uncertain if you should do so then check with the St Peter's data protection lead.

When using personal data you must not write comments about the individual that are unfair, untrue or offensive that you would not be able to defend. This includes emails

In the event of a data breach

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. It is compulsory to inform the data protection lead at St Peter's immediately and the information governance officer (IGO) at the Diocese within 72 hours of discovering the breach. More details can be provided after that 72 hours. In certain circumstances, the individual affected will be informed eg if it puts the individual at high risk.

Contracts with suppliers and the data sharing agreement

It is compulsory that all third party suppliers who are processing data on behalf of St Peter's must only do so through the contract and make sure it is compliant. The contract must state that the processor must:

- Only act on written instructions of the data controller
- Their staff or others who are processing the data are subject to a duty of confidentiality
- Ensure the process is done securely

- Only engage a sub-processor with prior consent from St Peter's and with a written contract eg Mailchimp, Monkey survey, block emails by an outside mailing company
- Assist St Peter's to provide subject access and respond to other individual rights requests
- Assist St Peter's to make notification of personal data breaches
- Assist St Peter's to complete data protection impact assessments if required
- Delete or return all personal data if requested at the end of the contract
- Submit to audits and inspections
- Tell St Peter's immediately if asked to do anything that contravenes data protection law

If legal advice is required for any of these compliances the Diocesan Registrar should be contacted.

Penalties for non-compliance

Fines are a last resort and are most likely to be used where organisations systematically fail to comply with the law or completely disregard it. It is likely that in a breach the commitment will be to help the organisation to comply.

Approved by:

Date

Date for renewal

References:

Church of England Data Protection Policy 2018

St Peter's Safeguarding policy 2017

Documents relating to GDPR and employment can be found under employment on the St. Peter's website

Appendix 1 Checklist

ACTION NEEDED

THE CHURCH OF ENGLAND

GDPR CHECKLIST

The General Data Protection Regulation (GDPR) will take effect in the UK in May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection in how their personal data is used by organisations. Parishes must comply with its requirements, just like any other charity or organisation. Use this handy checklist to make sure you're on top of what you need to do. See also our guidance at *www.parishresources.org.uk/gdpr*

The Checklist	*Sorted*	*Action needed & date completed*
1 **Data Audit** Use our template to review your data processing. This is a great first step to identify the other action you will need to take. We've provided a template at *www.parishresources.org.uk/gdpr/dataaudit*	☐	
2 **Privacy Notice:** Have you drafted a Privacy Notice. You can find guidance and a sample template at: *www.parishresources.org.uk/gdpr/privacy*	☐	
Is it available online for people to access?	☐	
Is there a date set to review it?	☐	
3 **Do you need to get additional consent....** It's likely that many parishes will need to get additional consent from people as either consent has been assumed, or the evidence of the consent is no longer available. See our example consent forms at *www.parishresources.org.uk/gdpr/consent*	☐	
4 **Are your procedures up to date?** Data subjects (those people about whom you hold personal data) have the right to see what data is being stored about them, to make corrections where there are errors, or to ask for their data to be deleted. Do you have processes in place to meet such requests?	☐	
5 **What if you had a breach** Review your breach management procedures and ensure that you know what to do in the event of a breach. If you don't have any, you will need to develop them. See our guide at *www.parishresources.org.uk/gdpr*	☐	

www.parishresources.org.uk/gdpr

Appendix 2

DATA PRIVACY NOTICE

The Parochial Church Council (PCC) of St Peter's Church Wellesbourne covering Incumbent, Curate and Readers

1. Your personal data – what is it?
2. Who are we?
3. How do we process your personal data?

   Personal data relates to a living individual who can be identified from that data.

   Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession.

   The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

   The PCC of St Peter's Wellesbourne, the Incumbent, Assistant Ministers and Office Administrator are the data controllers (contact details below). This means they decide how your personal data is processed and for what purposes.

   All mentioned above complies with its obligations under the "GDPR" by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

   We use your personal data for the following purposes: -

   To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution;

   To administer membership records;

   To fundraise and promote the interests of the charity;

   To manage our employees and volunteers;

   To maintain our own accounts and records (including the processing of gift aid applications);

   To inform you of news, events, activities and services running at St Peter's;

   To share your contact details with the Diocesan office so they can keep you informed about news in the diocese and events, activities and services that will be occurring in the diocese and in which you may be interested.

4. What is the legal basis for processing your personal data?

   Explicit consent of the data subject so that we can keep you informed about news, events, activities and services and process your gift aid donations and keep you informed about diocesan events.

   Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement;

   Processing is carried out by a not-for-profit body with a religious aim provided: - the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and there is no disclosure to a third party without consent.

5. Sharing your personal data

   Your personal data will be treated as strictly confidential and will only be shared with other members of the church in order to carry out a service to other church members or for purposes connected with the church.

   We will only share your data with third parties outside of the church with your consent.

6. How long do we keep your personal data?

   Your personal data will be treated as strictly confidential and will only be shared with other members of the church in order to carry out a service to other church members or for purposes connected with the church. We will only share your data with third parties outside of the parish with your consent.

   We keep data in accordance with the guidance set out in the guide “Keep or Bin: Care of Your Parish Records” which is available from the Church of England website (Details about retention periods can currently be found in the Record Management Guides located on the Church of England website at: -https://www.churchofengland.org/more/libraries-and-archives/records-management-guides)

   Specifically, we retain electoral roll data while it is still current; gift aid declarations and associated paperwork for up to 7 years after the tax year to which they relate; and parish registers (baptisms, marriages, funerals) permanently.

7. Your rights and your personal data

   Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

   The right to request a copy of your personal data which we hold about you;

   The right to request that we correct any personal data if it is found to be inaccurate or out of date;

   The right to request your personal data is erased where it is no longer necessary for us to retain such data;

   The right to withdraw your consent to the processing at any time;

   The right to request that the data controller provide the data subject with their personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable) [This only applies where the processing is based on consent or is necessary for the performance of a contract with the data subject and in either case the data controller processes the data by automated means].

   The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request that a restriction is placed on further processing;

   The right to object to the processing of personal data, (where applicable) [Only applies where processing is based on legitimate interests (or the performance of a task in the public interest/exercise of official authority); direct marketing and processing for the purposes of scientific/historical research and statistics]

   The right to lodge a complaint with the Information Commissioners Office.

   If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Contact Details

To exercise all relevant rights, queries of complaints please in the first instance contact the St Peter’s parish office via email st.p.wellesbourne@gmail.com

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office,

Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF

Appendix 3

St Peter's Wellesbourne

CONSENT FORM

Your privacy is important to us, and we want to communicate with church members in a way which has their consent, and which is in line with UK law on data protection. As a result of a change in UK law, we now need your consent to how we contact you. Please fill in the contact details you want us to use to communicate with you:

Name _____
Address: _____
_____
Email Address: _____
Phone Number landline: _____
Mobile number: _____
Social Media (state app.) _____

By signing this form you are confirming that you are consenting to the PCC of St Peter's Wellesbourne holding and processing your personal data for the following purposes (please tick the boxes where you grant consent):-

I consent to the church contacting me by;

☐post ☐landline phone ☐mobile phone ☐email ☐social media.

☐To keep me informed about news, events, activities, stewardship, fund raising, deanery, pastoral concerns and services at St Peter's

☐To including my details in the 'Church Directory' which is circulated to Church Members.

☐To share my contact details with the Diocese of Coventry so they can keep me informed about news, events, activities and services that will be occurring in the diocese and which are directly relevant to the role I am undertaking;

Signed:_____Dated: _____

You can grant consent to all the purposes; one of the purposes or none of the purposes. Where you do not grant consent we will not be able to use your personal data; (so for example we may not be able to let you know about forthcoming services and events); except in certain limited situations, such as where required to do so by law or to protect members of the public from serious harm. You can find out more about how we use your data from our "Privacy Notice" which is available from our website or from the Parish Office.
You can withdraw or change your consent at any time by contacting the Parish Administrator at St Peter's Church Office st.p.wellesbourne@gmail.com. Please note that all processing of your personal data will cease once you have withdrawn consent, other than where this is required by law, but this will not affect any personal data that has already been processed prior to this point.

St Peter's PCC is a Registered Charity, No 1143822

Appendix 4

Legitimate Interest Assessment

When can you rely on legitimate interests?

- When processing is not required by law but is of benefit to you
- When there is a limited privacy impact on the data subject
- When the data subject would reasonably expect your processing to take place

In order to use legitimate interests as your lawful basis for processing, your processing must therefore meet all of the following criteria:

- Have a specific purpose with a defined benefit
- Be necessary – if your defined benefit can be achieved without processing personal data then legitimate interests is not appropriate
- Be balanced against, and not override, the interests, rights and freedoms of data subjects

For further information and assistance seek advice from [*the DPO or Data Protection Lead or local registrar as appropriate]*.

Appendix 5

Criminal Offences	Only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.
	Must have both a lawful basis and either legal authority or official authority for the processing. You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this.

Appendix 6 Flow Chart of Process